helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

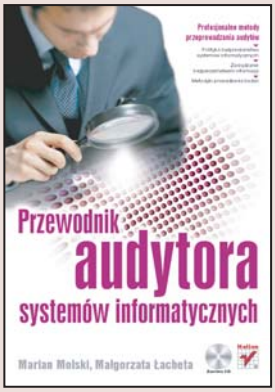
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

# Przewodnik audytora systemów informatycznych




Autorzy: Marian Molski, Małgorzata Łacheta
ISBN: 83-246-0622-X
Format: A5, stron: 424

Dynamiczny rozwój technologii informatycznych znacząco wpłynął na konkurencyjność i efektywność organizacji. Bez odpowiedniego wsparcia ze strony systemów informatycznych współczesne przedsiębiorstwo nie jest w stanie poprawnie funkcjonować. Jednak tak duże uzależnienie od systemów informatycznych oznacza również zagrożenia związane z możliwością utraty bądź wykradzenia kluczowych danych firmy. Wirusy, programy szpiegujące, działania hakerów – wszystko to może spowodować ogromne straty dla organizacji. Na szczęście zwiększa się również arsenał narzędzi, dzięki którym firmy mogą bronić się przed takimi zagrożeniami. Jak jednak stwierdzić, czy przedsięwzięte środki ochrony są wystarczające?

Czytając książkę „Przewodnik audytora systemów informatycznych", poznasz procedury i praktyczne zagadnienia związane z badaniem infrastruktury informatycznej pod tym właśnie kątem. Dowiesz się, czym dokładnie zajmuje się audytor systemów informatycznych i jak planuje się korporacyjną politykę bezpieczeństwa danych. Przeczytasz o planowaniu badań oraz narzędziach i metodykach wykorzystywanych w tym procesie. Nauczysz się przeprowadzać analizę systemów informatycznych i dowiesz się, na co zwracać szczególną uwagę.

- Elementy polityki bezpieczeństwa danych
- Zarządzanie ryzykiem w systemach informatycznych
- Wdrożenie systemu zarządzania bezpieczeństwem informacji
- Model PDCA
- Regulacje prawne i standardy związane z audytem
- Metodyki prowadzenia badań systemów informatycznych
- Przeprowadzanie procesu audytu

**Audytor systemów informatycznych to zawód przyszłości.**
**Bądź przygotowany na jej nadejście**

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

# Spis treści

**O autorach** ..... **7**

**Od autorów** ..... **9**

**Wstęp — dla kogo, w jakim celu?** ..... **11**

**Audyt systemów informatycznych — uwagi wprowadzające** ..... **17**

Geneza ..... 23

Organizacje zawodowe ..... 25

Certyfikacja ..... 29

Rynek usług ..... 35

Pytania do rozdziału 2. ..... 41

**Słownik terminów związanych z audytem systemów informatycznych** ..... **43**

Wersja polsko-angielska ..... 44

Wersja angielsko-polska ..... 59

**Wprowadzenie do zarządzania bezpieczeństwem systemów informatycznych** ..... **75**

Elementy bezpieczeństwa ..... 76

Polityka bezpieczeństwa ..... 83

Pytania do rozdziału 4. ..... 85

**Procesy zarządzania bezpieczeństwem systemów informatycznych** ..... **87**

Zarządzanie konfiguracją ..... 88

Zarządzanie zmianami ..... 89

Zarządzanie ryzykiem ....90
Pytania do rozdziału 5. ....103

**System zarządzania bezpieczeństwem informacji .... 105**
Ustanowienie ISMS ....106
Wdrożenie i eksploatacja ....108
Monitorowanie i przegląd ....108
Utrzymanie i doskonalenie ....109
Wymagania dotyczące dokumentacji ....109
Przegląd realizowany przez kierownictwo ....110
Pytania do rozdziału 6. ....112

**Model PDCA w procesach ISMS .... 113**
Faza planowania ....114
Faza wykonania ....115
Faza sprawdzania ....116
Faza działania ....118
Pytania do rozdziału 7. ....119

**Wprowadzenie do audytowania .... 121**
Statut audytu — prawa i powinności audytora ....126
Kodeks Etyki Zawodowej ....127
Klasyfikacja audytów ....128
Porównanie kontroli, audytu i controllingu ....155
Pytania do rozdziału 8. ....158

**Standaryzacja w audycie i bezpieczeństwie systemów informatycznych .... 159**
Regulacje prawne ....161
Standardy typu best practice ....169
Standardy umożliwiające certyfikację ....193
Pytania do rozdziału 9. ....210

**Przegląd znanych metodyk prowadzenia audytu systemów informatycznych .... 213**
COBIT ....214
LP-A ....239
MARION ....251

OSSTM ..... 252
TISM ..... 261
Pytania do rozdziału 10. ..... 272

**Wykonanie audytu ..... 275**
Obiekty, zakres i cel ..... 277
Fazy audytu ..... 282
Zawartość dokumentacji ..... 282
Dowody audytowe ..... 292
Proces audytowy ..... 297
Pytania do rozdziału 11. ..... 315

**Planowanie długoterminowe ..... 319**
Ocena potrzeb audytu ..... 320
Roczny plan audytu ..... 322
Plan strategiczny ..... 324
Pytania do rozdziału 12. ..... 325

**Planowanie ciągłości działania ..... 327**
Rola audytu w planowaniu ciągłości działania ..... 328
Metodyka audytowania planu ciągłości działania ..... 330
Pytania do rozdziału 13. ..... 337

**Wykorzystanie oprogramowania narzędziowego w audycie ..... 339**
Komputerowe techniki wspomagania audytu ..... 340
Wymagania standardów ..... 351
Klasyfikacja programów wspomagających audyt ..... 355
Pytania do rozdziału 14. ..... 357

**Podsumowanie ..... 359**

**Literatura ..... 361**

**Źródła internetowe ..... 375**

**Odpowiedzi do pytań testowych ..... 405**

**Skorowidz ..... 407**

# 11
# Wykonanie audytu

W celu poprawnego przeprowadzenia audytu ważne jest, by zastosować właściwą metodykę (rozdział 10.) oraz odpowiednio wskazać zakres i obiekty badania. Ścisła integracja systemów informatycznych i procesów biznesowych przy ciągłym wzroście złożoności tych systemów oraz szybkim tempie zmian biznesowych sprawia, że niemal każdy element środowiska informatycznego jednostki może stać się obiektem audytu. Techniką przydatną do poprawnego wykonania przeglądu jest podejście wykorzystujące analizę ryzyka (rozdział 5.). Dzięki zastosowaniu tego rozwiązania audytor ma pewność, że bada obszary obarczone najwyższym ryzykiem materializacji zagrożenia.

Odmiennym sposobem prowadzenia audytu jest ocena całego środowiska i systemów operacyjnych jednostki. Rozwiązanie to nazywane jest często starym modelem audytowania (tabela 11.1).

Audytor powinien zdefiniować zbiór procesów, by wyznaczyć obiekty kontroli, zebrać i przeanalizować dowody oraz opracować wnioski oraz rekomendacje w ramach raportowania.

W celu poprawnej realizacji audytu należy wykonać następujące czynności:

1. zaplanować spotkanie audytowe;
2. stworzyć procedury audytu z uwzględnieniem oszacowanego poziomu ryzyka nieregularnych i nielegalnych zdarzeń;
3. założyć, że zdarzenia te nie są odosobnione;

**Tabela 11.1.** *Porównanie starego (tradycyjnego) modelu audytowania i nowoczesnego podejścia wykorzystującego analizę ryzyka*

| Proces audytu | Audyt nowoczesny | Audyt tradycyjny |
|---|---|---|
| Rodzaje audytów | Podział na audyt projektów i ciągły proces audytowy | Wyróżnia się audyt finansowy, operacyjny, informatyczny i zgodności |
| Obszar audytu | Wszystkie systemy, za pomocą których realizowane są cele biznesowe, zidentyfikowane są w badanej jednostce | W pierwszej kolejności aydytowana jest działalność operacyjna i zgodność z prawem |
| Cele audytu | Określenie, czy ryzyko zostało ograniczone do dopuszczalnego poziomu | Ocena systemu kontroli wewnętrznej pod kątem jego efektywności i wydajności |
| Planowanie | Wybór zadań audytowych z wykorzystaniem analizy ryzyka | Plany audytów niekoniecznie muszą być powiązane z analizą ryzyka |
| Zaangażowanie pracowników jednostki | Wysoki stopień zaangażowania pracowników jednostki audytowanej we wszystkich fazach audytu | Zaangażowanie niewielkie, zwykle dotyczy tylko zapoznania z programem audytowym, wstępnej oceny raportu, potwierdzenia zawartych w raporcie końcowym wniosków i rekomendacji |
| Realizacja audytów | Możliwość równoczesnego wykonywania kilku zadań audytowych | Audytor realizuje zadania audytowe kolejno jedno po drugim |
| Cele testowania | Znalezienie błędów funkcjonowania systemu kontroli oraz wykorzystanie analizy ryzyka do określenia, które nieprawidłowości są najważniejsze i wymagają oceny | Znalezienie błędów funkcjonowania systemu kontroli bez uwzględniania ich istotności |
| Raportowanie | Zapewnienie podmiotu zlecającego audyt, że wszystkie rodzaje ryzyka znajdują się na akceptowalnym poziomie, oraz wskazanie tych rodzajów ryzyka, które należy ograniczyć | Potwierdzenie poprawności funkcjonowania systemu kontroli wewnętrznej oraz wskazanie jego ewentualnych słabości |

4. określić, w jaki sposób zdarzenia te omijają system kontroli wewnętrznej;
5. rozszerzyć procedury audytu, by wskazać prawdopodobieństwo wystąpienia innych tego typu zdarzeń;
6. opracować dodatkowe procedury audytowe;
7. ocenić wyniki rozszerzonych procedur audytowych;
8. skonsultować z zarządem znalezione defekty oraz oszacować potencjalny wpływ nielegalnych i nieregularnych zjawisk na organizację;
9. opracować raport obejmujący wszystkie zgromadzone fakty i okoliczności wystąpienia nieprawidłowości;
10. przekazać wyniki raportu właściwym przedstawicielom jednostki audytowanej (zarządowi, kierownikom zajmującym stanowiska przynajmniej o poziom wyższe w hierarchii zawodowej organizacji niż personel poddawany badaniu).

## Obiekty, zakres i cel

Audytor może poprawnie wykonywać czynności zawodowe tylko wtedy, gdy w pełni rozumie funkcje i cele biznesowe jednostki audytowanej. Bardzo istotną umiejętnością jest poprawne wskazanie obiektów, celów i zakresu badania zgodnie ze strategią działania organizacji.

Uniwersalnym ***celem audytu*** jest zapewnienie, że w badanym obszarze zadania wykonywane są efektywnie, wydajnie i zgodnie z prawem, a wszelkie odstępstwa podlegają raportowaniu. Na cele audytu systemów informatycznych mogą mieć wpływ:

- potrzeby zainteresowanych stron;
- planowany zakres rozpowszechnienia raportu;
- uregulowania prawne i standardy branżowe.

W praktyce audyt dla celów bezpieczeństwa teleinformatycznego przeprowadza się, aby [67]:

- wykazać, że informacja i system teleinformatyczny został zabezpieczony zgodnie z ustaleniami pomiędzy zleceniodawcą a zespołem budującym system bezpieczeństwa;
- wykazać, że system bezpieczeństwa spełnia wymagania norm i standardów w tym zakresie;
- wystawić ocenianemu systemowi tzw. certyfikat bezpieczeństwa (coraz częstsza praktyka ze względu na ustawę o ochronie informacji niejawnych, członkostwo Polski w NATO oraz wejście do Unii Europejskiej);
- ocenić jakość systemu zabezpieczeń i przedstawić opinię zleceniodawcy (modernizujemy lub zostawiamy bez zmian).

Cele wykonania audytu informatycznego to przede wszystkim [67]:

- weryfikacja zgodności działania systemów informatycznych z wymogami prawa (ustawa o rachunkowości, o ochronie danych osobowych itp. — por. rozdział 9.);
- weryfikacja stanu bezpieczeństwa systemów informatycznych oraz pojedynczych aplikacji z perspektywy występującego ryzyka (swobodna interpretacja terminów: ryzyko i analiza ryzyka może prowadzić do nieporozumień), a także zaimplementowanych procedur kontrolnych i ich efektywności;
- analiza ryzyka związanego z prowadzeniem projektu informatycznego.

Przytoczone wnioski pozwalają zatem wskazać, co nie jest celem audytu systemów informatycznych:

- sprawdzanie zapisów w dziennikach systemowych,
- sprawdzanie konfiguracji stacji roboczych.

***Obiekty audytu*** to fragmenty zadania audytowego (np. podsystemy badanego systemu). Powinny one zostać zidentyfikowane przez audytora w taki sposób, by możliwe było opisanie ich w raporcie. Ważne jest wskazanie obiektów istotnych dla realizacji celów audytu.

**Wskazówka!**

Zadanie audytowe — **odpowiedni podział procesów zidentyfikowanych w ramach danej jednostki. Wyodrębnia się tu:**

- **cel audytu,**
- **zakres przedmiotowy badań — obiekty audytu,**
- **zakres podmiotowy przeglądu — jednostki audytowane.**

**Przykładowe obiekty audytu systemów informatycznych:**

1. Bezpieczeństwo i integralność danych
2. Plany ciągłości działania
3. Procedury zakupu sprzętu i oprogramowania
4. Utrzymanie oraz serwis sprzętu i oprogramowania
5. Zarządzanie zmianami
6. Zarządzanie jakością
7. Ocena systemu kontroli
8. Zgodność z uregulowaniami prawnymi i normatywnymi
9. Zarządzanie personelem działu informatycznego
10. Zarządzanie projektami informatycznymi

***Zakres audytu*** powinien obejmować system kontroli użytkowania i ochrony zasobów informatycznych, a także procesy dotyczące planowania, organizowania i monitorowania środowiska informatycznego jednostki. Ważne jest, by uwzględnić zależność pomiędzy nakładem pracy a istotnością obiektów audytu. W celu właściwego ustalenia zakresu badania audytor powinien wykorzystać profesjonalny osąd.

Zadaniem audytora jest również ustalenie ***obiektów kontroli***. W odróżnieniu od obiektów audytu, które są samodzielnie opracowywane przez audytora, obiekty kontroli powinny zostać wcześniej zdefiniowane przez kierownictwo. Ocena obiektów kontroli polega na sprawdzeniu, czy zastosowane kontrole zapewniają realizacje celów badanego systemu. Audytor powinien rozumieć różnicę między obiektami audytu a kontrolą. Obiekty audytu to obszary objęte przeglądem;

obiekty kontroli dotyczą badanego systemu i wskazują cele działań kontrolnych.

W tabeli 11.2 przedstawiono przykładową macierz kontrolną, czyli obiekty kontroli, związane z nimi czynności kontrolne i procedury audytowe.

**Tabela 11.2.** *Przykładowa macierz kontrolna (opracowanie własne [56])*

| Obiekty kontroli | Czynności kontrolne | Procedury audytowe |
|---|---|---|
| ***Niezależne przeglądy prowadzone przez kierownictwo*** | | |
| Kierownictwo powinno przeprowadzać okresowe niezależne przeglądy (w tym audyty wewnętrzne i zewnętrzne) operacji informatycznych, by zapewnić, że odpowiednie polityki oraz procedury zostały właściwie wdrożone i działają efektywnie | Kierownictwo ustala harmonogram okresowych niezależnych przeglądów operacji informatycznych, a także formalne procedury dotyczące działań naprawczych po wykryciu nieprawidłowości | Ocenić zaimplementowane polityki i procedury oraz harmonogram niezależnych wewnętrznych przeglądów, by sprawdzić, czy zapewniają one niezależne przeglądy operacji informatycznych i właściwe działania naprawcze zidentyfikowanych słabości systemu |
| ***Organizacja*** | | |
| Obowiązki i odpowiedzialność powinny być rozdzielone w taki sposób, by żadna osoba nie mogła popełnić ani ukryć istotnych błędów | Kierownictwo zapewnia odpowiedni rozdział obowiązków i określa zakres odpowiedzialności w dziale informatycznym, by uniknąć popełniania i ukrywania błędów | Ocenić strukturę organizacyjną jednostki w celu sprawdzenia, czy dział informatyczny funkcjonuje na wystarczająco wysokim poziomie w hierarchii służbowej, by jego działania było niezależne<br>Sprawdzić, czy obowiązki i odpowiedzialność są właściwie rozdzielone pomiędzy pracowników działu informatycznego |

**Tabela 11.2.** *Przykładowa macierz kontrolna (opracowanie własne [56]) — ciąg dalszy*

| Obiekty kontroli | Czynności kontrolne | Procedury audytowe |
|---|---|---|
| ***Nabywanie, rozwijanie i modyfikowanie oprogramowania*** | | |
| Kierownictwo powinno zwracać szczególną uwagę na właściwe zarządzanie oprogramowaniem. Wykorzystywane oprogramowanie musi być zgodne ze specyfikacjami i niewrażliwe na nieuprawnioną modyfikację, a przed wdrożeniem musi być poddane odpowiednim testom | Kierownictwo ustanawia i utrzymuje standardową metodykę zawierającą następujące elementy kontrolne:<br>• wykaz pisemnych wymagań zaakceptowany przez kierownictwo i użytkowników aplikacji<br>• udział odpowiednich członków personelu (kierownictwo i użytkownicy) we wszystkich fazach nabywania, utrzymywania i modyfikowania oprogramowania<br>• odpowiednia dokumentacja wszystkich wykorzystywanych programów<br>• zatwierdzanie, weryfikacja oraz testowanie oprogramowania przez kierownictwo i odpowiednich członków personelu działu informatycznego, by potwierdzić, że działa ono zgodnie ze specyfikacjami i wymaganiami klientów<br>• ostateczne pisemne zatwierdzenie aplikacji (przed implementacją oprogramowania) przez kierownictwo, personel działu informatycznego i użytkowników | Jeśli z oceny ryzyka wynika, że konieczne są w tym obszarze dalsze działania audytowe, należy przeprowadzić ocenę przynajmniej jednego projektu zakupu, rozwijania i modernizacji oprogramowania, by wskazać, czy:<br>• pisemne wymagania zostały zatwierdzone przez kierownictwo i wskazanych użytkowników,,<br>• odpowiedni przedstawiciele kierownictwa i działu informatycznego uczestniczą we wszystkich fazach uzyskiwania, rozwijania i modyfikacji oprogramowania<br>• wszystkie programy są odpowiednio udokumentowane<br>• kierownictwo i odpowiedni członkowie personelu działu informatycznego zatwierdzili, zweryfikowali oraz przetestowali oprogramowanie pod kątem zgodności ze specyfikacjami i wymaganiami klientów<br>• przed wdrożeniem oprogramowania zostało wydane pisemne zatwierdzenie aplikacji przez kierownictwo, personel działu informatycznego i użytkowników |

## Fazy audytu

W rozdziale 10. przedstawiono różne metodyki prowadzenia audytu. W ramach przypomnienia — metodyka to zbiór udokumentowanych procedur audytowych mających zapewnić, że audytor osiągnie zamierzone cele audytu. Przyjęta metodyka obejmuje wszystkie fazy przeglądu (tabela 11.3) i umożliwia wypracowanie powtarzalnego, stałego podejścia do audytu w jednostce. Metodyka powinna być udokumentowana oraz zatwierdzona przez dyrektora zespołu audytowego. Należy zapoznać wszystkich członków zespołu z przyjętą strategią działań.

Wykorzystanie metodyki audytu pozwala opracować zakres audytu, zapewnia stałość oraz powtarzalność procesów, wskazuje szczegółowe działania, niezbędne do prawidłowej realizacji przeglądu. Dodatkowo, dzięki takiemu schematycznemu podejściu działania audytowe pozostawiają udokumentowany ślad tego, co zostało objęte badaniem oraz tego, z kim przeprowadzono wywiady, jakie zebrano dowody i w jaki sposób wykonano testy mechanizmów kontrolnych. Wszystko to sprawia, że raport z badania jest kompletny, nie dochodzi do przekroczenia zakresu audytu oraz że osiągnięte zostają zamierzone cele przeglądu.

## Zawartość dokumentacji

Dokumentacja audytu systemów informatycznych jest zapisem przeprowadzonych przez audytora czynności oraz dowodem potwierdzającym sformułowane wnioski i rekomendacje.

Dokumentacja audytu powinna zawierać informacje dotyczące:

- zakresu i celów audytu,
- programu audytu,
- kolejno wykonywanych działań w ramach przeglądu,
- zgromadzonych dowodów,
- wniosków i rekomendacji będących produktem audytu,

**Tabela 11.3.** *Fazy typowego audytu (opracowanie własne na podstawie [56])*

| | |
|---|---|
| **Temat audytu** | Identyfikacja obszaru (obszarów) audytu |
| **Cele audytu** | Wskazanie powodów, dla których przeprowadza się audyt. Przykładowo, celem audytu może być zapewnienie, że dostęp do własności intelektualnych jest właściwie kontrolowany |
| **Zakres audytu** | Identyfikacja objętych przeglądem systemów lub funkcji organizacji |
| **Faza I**: Planowanie | Określenie potrzebnych zasobów ludzkich (w tym osób z wiedzą specjalistyczną) i materialnych (laptopy, oprogramowanie wspomagające audyt)<br>Identyfikacja źródeł informacyjnych — polityki, procedur, planów projektowych, logów<br>Wskazanie lokalizacji lub obiektów objętych audytem |
| **Faza II**: Procedury audytowe i etapy gromadzenia informacji | Identyfikacja i wybór procesu do weryfikacji oraz przeprowadzanie testów mechanizmów kontrolnych<br>Wskazanie osób do przeprowadzenia wywiadów<br>Identyfikacja i zdobycie potrzebnych polityk oraz standardów<br>Opracowanie procedur audytowych do przeprowadzenia weryfikacji i testów kontrolnych |
| **Faza III**: Procedury do oceny wyników testów lub przeglądu | Identyfikacja procesu objętego przeglądem i ocena wyników audytu |
| **Faza IV**: Procedury prowadzenia rozmów z kierownictwem | Określenie procedur dotyczących sposobu przedstawienia raportu z audytu kierownictwu jednostki audytowanej<br>Opracowanie procedur dotyczących komunikowania się w trakcie działań audytowych |
| **Faza V**: Opracowanie raportu | Identyfikacja działań poaudytowych<br>Wskazanie procedur służących do oceny efektywności i wydajności operacyjnej<br>Identyfikacja procedur dotyczących testów mechanizmów kontrolnych<br>Przegląd i ocena znaczących dokumentów, polityk i procedur |

- opracowanych raportów,
- przeglądu działań audytora dokonywanych przez kierownictwo.

Bardzo ważne jest, by dokumentacja była kompletna, czytelna i zrozumiała dla osób, do których jest adresowana.

Nie należy również zapominać o odpowiednim zabezpieczeniu i przechowywaniu dokumentacji. W tym celu powinna zostać opracowana oraz wdrożona polityka i procedury właściwego zarządzania (zabezpieczania, przechowywania, odzyskiwania) dokumentacją.

## Dokumenty robocze

Wszelkie wnioski sformułowane na podstawie działań audytowych muszą być poparte odpowiednimi dowodami. Najlepszym potwierdzeniem prawdziwości ustaleń jest powołanie się na dokumenty robocze (***cross check***). Nie istnieje obowiązek powoływania się w treści raportu na wszystkie dokumenty robocze audytu.

Dokumenty robocze tworzy się w celu:

- udokumentowania zrealizowanych działań,
- potwierdzenia prawdziwości sformułowanych wniosków,
- umożliwienia przeprowadzenia kontroli realizacji działań audytowych,
- usprawnienia wykonywanych czynności.

Każdy dokument roboczy opatrzony jest nagłówkiem z nazwą jednostki audytowanej, tytułem, celem i datą sporządzenia. Ponadto, powinien posiadać on swój unikatowy (w ramach danego audytu) numer referencyjny i być podpisany przez audytora (np. poprzez umieszczenie inicjałów osoby prowadzącej przegląd). Należy również pamiętać o odpowiednim wyjaśnieniu skrótów i symboli, zastosowanych w ramach danego dokumentu roboczego, oraz o precyzyjnym wskazaniu źródeł informacji.

Za prawidłowość zgromadzonej dokumentacji roboczej odpowiedzialny jest dyrektor zespołu audytowego i koordynator zadania audytowego.

Najczęściej stosowane dokumenty robocze to:

1. **Kwestionariusz kontroli wewnętrznej (KKW)**

   KKW to dokument zawierający pytania dotyczące systemu kontroli wewnętrznej, które mają pomóc w jego ocenie. Uzyskane w ten sposób informacje powinny być dodatkowo potwierdzone

dowodami pochodzącymi z innych źródeł. Audytor może kierować do kierownictwa i personelu jednostki audytowanej pytania otwarte i zamknięte.

Pytania zamknięte posiadają tylko dwa warianty odpowiedzi: TAK lub NIE. Pomimo że przygotowanie tego rodzaju pytań jest pracochłonne, daje jednak możliwość szybkiej analizy otrzymanych odpowiedzi i zdobycia informacji na temat systemu kontroli wewnętrznej oraz wiarygodności audytowanych.

Pytania otwarte w żaden sposób nie ograniczają audytowanych, pozwalają na swobodny sposób przedstawienia zdarzeń i relatywnie łatwo można je opracować. Niestety, wiedza zdobyta w ten sposób daje jedynie obraz zasad funkcjonowania badanego systemu kontroli.

Należy pamiętać, że KKW powinien być stosowany w początkowej fazie audytu, by istniała możliwość potwierdzenia zgromadzonych przy jego użyciu informacji w trakcie dalszych działań audytowych. Przykładowy kwestionariusz kontroli wewnętrznej przedstawiony został w tabeli 11.4.

**Tabela 11.4.** *Przykładowy kwestionariusz kontroli wewnętrznej dla audytu planowania ciągłości działania*

Kwestionariusz kontroli wewnętrznej

Nazwa zadania audytowego: Audyt planowania ciągłości działania

Numer zadania audytowego:.....

Wykonał:.....
Data:.....

Sprawdził: .....
Data:.....

| Lp. | Pytanie | TAK | NIE | ND |
|---|---|---|---|---|
| 1. | Czy zdefiniowano politykę jednostki w zakresie planowania ciągłości działania? | | | |
| 1.1 | Czy określono odpowiedzialność za planowanie ciągłości działania i zarządzanie kryzysowe? | | | |
| 1.2 | Czy wskazano warunki uznania sytuacji za kryzysową? | | | |
| 1.3 | Czy określono ogólne zasady postępowania w sytuacji kryzysowej? | | | |

**Tabela 11.4.** *Przykładowy kwestionariusz kontroli wewnętrznej dla audytu planowania ciągłości działania — ciąg dalszy*

| Lp. | Pytanie | TAK | NIE | ND |
|---|---|---|---|---|
| 1.4 | Czy określono sposób zarządzania jednostką w sytuacji kryzysowej? | | | |
| 1.5 | Czy zostały określone krytyczne zasoby dla funkcjonowania jednostki? | | | |
| 2. | Czy zostały opracowane plany ciągłości działania? | | | |
| 2.1 | Czy plany ciągłości działania szczegółowo określają zadania, które muszą być zrealizowane w sytuacji kryzysowej? | | | |
| 2.2 | Czy określono zespoły realizujące plany ciągłości działania? | | | |
| 2.3 | Czy plan ciągłości działania obejmuje fazę początkową (powiadomienie i aktywację)? | | | |
| 2.4 | Czy plan ciągłości działania obejmuje fazę odtworzenia krytycznych funkcji biznesowych? | | | |
| 2.5 | Czy plan ciągłości działania obejmuje fazę przywrócenia normalnego funkcjonowania jednostki? | | | |
| 2.6 | Czy zdefiniowano zasady ochrony poufności planów ciągłości działania? | | | |
| 2.7 | Czy wdrożono strategię przeprowadzania testów planów ciągłości działania? | | | |
| 3. | Czy została opracowana strategia utrzymania dostępności zasobów w sytuacji kryzysowej? | | | |
| 4. | Czy określono i wdrożono politykę informacyjną w przypadku wystąpienia sytuacji kryzysowej? | | | |
| 5. | Czy wdrożono proces weryfikacji zasad związanych z zapewnieniem ciągłości działania? | | | |
| 5.1 | Czy weryfikacja przeprowadzana jest okresowo? | | | |
| 5.2 | Czy weryfikacja przeprowadzana jest po wystąpieniu istotnych zmian w jednostce? | | | |
| 5.3 | Czy podstawą do weryfikacji są wyniki analizy ryzyka? | | | |
| 5.4 | Czy weryfikacja przeprowadzana jest z udziałem zewnętrznych ekspertów? | | | |
| Odpowiedzi udzielił:.....<br>Audytowany:.....<br>Audytorzy:..... | | | | |

2. **Lista kontrolna** (*check list*)

   Dokument ten ma wszechstronne zastosowanie i może być wykorzystywany na każdym etapie realizacji procesu audytowego. Lista kontrolna pomaga w ujednoliceniu zdobytych informacji, umożliwia standardowe podejście do przeprowadzanego badania i zapobiega pominięciu istotnych kontroli. Listy kontrolne mogą być stosowane przez audytora i audytowanych. Z punktu widzenia audytu istotny jest sposób wykonywania i rejestrowania czynności nadzorczych. Listy kontrolne powinny zawierać rubryki wypełniane przez pracownika jednostki oraz przez kierownika nadzorującego daną czynność. Zadaniem audytora jest ustalenie, czy nadzór jest rzeczywiście realizowany, czy też jest to tylko kwestia formalna.

3. **Kwestionariusz samooceny**

   Kwestionariusz samooceny ma podobny układ jak KKW. W tym przypadku dokument wypełniany jest samodzielnie przez kierownictwo jednostki audytowanej, a pytania dotyczą rodzajów ryzyka związanych z działalnością organizacji. Narzędzie to powinno być stosowane w początkowej fazie audytu, gdyż wymaga potwierdzenia zgromadzonych danych przez inne źródła informacji.

4. **Plan kontroli**

   Plan kontroli służy do oceny systemu kontroli wewnętrznej i stanowi swoistą mapę pokazującą wszystkie kontrole zastosowane w danym systemie. Dokument ten określa zależności pomiędzy procedurami, wymaganiami standardów, ustaw i norm branżowych w odniesieniu do zastosowanych mechanizmów kontrolnych. Ponadto, plan kontroli wskazuje osoby odpowiedzialne za poszczególne kontrole, a także określa źródło ich opisu.

   Projektując systemy zarządzania, należy pamiętać, że wprowadzenie określonych wymagań narzuca konieczność wdrożenia mechanizmów kontrolnych ich realizacji. Plany kontroli są niezwykle przydatne przy planowaniu i dokumentowaniu testów zgodności. Przykładowy plan kontroli przedstawiony został w tabeli 11.5.

5. **Ścieżka audytu**

   Konieczność tworzenia ścieżki audytu dla środowiska informatycznego jest wywołana:

**Tabela 11.5.** *Przykładowy plan kontroli wewnętrznej — ochrona stanowiska pracy*

| **Plan kontroli** | | | | | | |
|---|---|---|---|---|---|---|
| **Lp.** | **Wymagania** | **Przepis** | **Jednostka odpowiedzialna** | **Pracownik odpowiedzialny** | **Opis kontroli** | **Dokument związany** |
| 1. | W jednostce została wdrożona zasada czystego biurka (nośniki informacji przechowywane są w zamkniętych szafach) | | | | | |
| 2. | W jednostce została wdrożona zasada czystego ekranu (otwarte są tylko te programy, z których użytkownik aktualnie korzysta) | | | | | |
| 3. | Stacje robocze są zabezpieczone hasłami przed nieuprawnionym dostępem | | | | | |
| 4. | Wskazano osoby, które mają dostęp do BIOS-u stacji roboczych | | | | | |
| 5. | Zdefiniowano zasady przechowywania i użytkowania haseł do BIOS-u | | | | | |
| 6. | Stacje robocze są wyposażone w wygaszasz ekranu | | | | | |
| 7. | Odblokowanie wygaszacza ekranu wymaga wprowadzenia hasła | | | | | |
| 8. | Wdrożono procedury blokowania przez użytkowników stacji roboczych przed odejściem od stanowiska pracy | | | | | |
| 9. | Procedury regulują ograniczenia w dostępie do danych w zależności od stażu pracy użytkownika | | | | | |
| 10. | Stacje robocze zostały pozbawione urządzeń umożliwiających nagranie informacji (napędu dyskietek, nagrywarki CD, nagrywarki DVD) | | | | | |
| 11. | Wprowadzono wydzielone (niepodłączone do sieci teleinformatycznej lub podłączone do sieci wydzielonej) stacje robocze wykorzystywane do przetwarzania informacji szczególnie wrażliwych | | | | | |
| 12. | Stacje robocze, o których mowa w punkcie 11., znajdują się w pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych | | | | | |

- dużą liczbą transakcji przetwarzanych w systemach informatycznych,
- ograniczonym do określonego przedziału czasu lub istniejącym tylko w czasie rzeczywistym zapisem operacji.

W skład ścieżki audytu wchodzą:

- system rejestrów (logów), w których zapisywane są wszystkie czynności użytkowników systemu,
- procedury i osoby odpowiedzialne za sprawdzenie informacji zapisanych w dziennikach,
- procedury kopiowania, przechowywania i zabezpieczania danych zawartych w dziennikach,
- narzędzia systemowe gwarantujące bezpieczeństwo i integralność danych.

Można wyróżnić kilka rodzajów rejestrów:

- rejestry transakcji,
- rejestry awarii i przestojów,
- rejestry błędów,
- rejestry bezpieczeństwa.

Wykorzystanie dzienników jest techniką skuteczną jedynie wtedy, gdy administrator regularnie tworzy kopie zapasowe. Rejestry mają bowiem ograniczoną pojemność i szybko się zapełniają, co prowadzi do utraty wcześniej zapisanych danych. Wszelkie zawarte w dziennikach informacje muszą być regularnie sprawdzane przez administratora systemu lub inną upoważnioną osobę.

Ścieżka audytu jest dokumentem szczególnie przydatnym dla:

- audytorów systemów informatycznych,
- administratorów systemów,
- administratorów bezpieczeństwa informacji.

Za brak właściwie opracowanej ścieżki audytu odpowiada kierownik organizacji. Stworzenie ścieżki audytowej wymaga zwykle przeprowadzenia prac audytowych, gdyż jest to jedyne narzędzie

umożliwiające zgromadzenie danych, niezbędnych do opracowania tego dokumentu.

W ramach podsumowania dokonano przeglądu najczęściej wykorzystywanych dokumentów roboczych (tabela 11.6).

## Techniki dokumentowania

Pierwszym etapem właściwego dokumentowania jest zrozumienie funkcji i charakteru badanego systemu oraz przetwarzanych w nim procesów. Przydatne do tego celu mogą okazać się następujące materiały:

- pisemne procedury,
- wyjaśnienia personelu obsługującego badany system,
- dokumenty z poprzednich audytów,
- przepisy,
- regulaminy,
- dokumenty opracowywane w trakcie przebiegu procesu.

Kolejny etap działań to wykorzystanie zgromadzonych materiałów do uzyskania określonych informacji. W tym momencie audytor powinien ustalić:

1. Jakie działania wchodzą w skład procesu?
2. Jaka jest kolejność tych czynności?
3. Kto wykonuje poszczególne działania budujące proces?
4. Jakie dokumenty są wykorzystywane w trakcie działania?
5. Jakie decyzje podejmowane są w trakcie wykonywania procesu?
6. Czy w realizacji procesu wykorzystywany jest system informatyczny, a jeśli tak, to jaki i w jakim zakresie?

Wszystkie wymienione informacje można zgromadzić, wykorzystując pisemne procedury. Badanie oparte wyłącznie na tych dokumentach jest jednak niewystarczające. W celu wyjaśnienia wszelkich wątpliwości dotyczących procesu wymagana jest współpraca z pracownikami, którzy go realizują.

**Tabela 11.6.** *Przegląd dokumentów roboczych*

| Lp. | Nazwa dokumentu | Opis |
|---|---|---|
| 1. | Zawiadomienie organizacji o rozpoczęciu prac audytowych | Dokument skierowany do kierownika organizacji, dotyczący terminu i zakresu badania |
| 2. | Protokół ze spotkania wstępnego | Dokumenty opracowywane w ramach zapoznania się z jednostką |
| 3. | Opis ustaleń z fazy wstępnej audytu | |
| 4. | Opis operacji wykonywanych przez organizację | |
| 5. | Plan audytu | Dokument opracowany we wstępnej fazie audytu; ma charakter ogólny |
| 6. | Macierz ryzyka | Narzędzie używane w analizie ryzyka |
| 7. | Program audytu | Dokument zawiera szczegółowy opis planowanych testów; przedstawione są w nim kolejne działania podejmowane w trakcie badania |
| 8. | Plany kontroli | Dokumenty identyfikujące wszystkie mechanizmy kontrolne zawarte w badanym systemie |
| 9. | Kwestionariusze kontroli wewnętrznej | Dokument zawierający pytania dotyczące istniejącego systemu kontroli wewnętrznej |
| 10. | Zapisy testów | Protokoły z wywiadów, wydruki komputerowe, kopie dokumentów, listy z potwierdzeniem pozytywnym |
| 11. | Kwestionariusze samooceny | Dokument wypełniany samodzielnie przez kierownictwo, mający zidentyfikować rodzaje ryzyka związanego z funkcjonowaniem jednostki audytowanej |
| 12. | Lista kontrolna | Dokument pozwalający na jednolite podejście realizacji działań audytowych |
| 13. | Ścieżka audytu | Dokument zawierający zestaw rejestrów z zapisanymi danymi na temat wykonywanych w systemie działań oraz odpowiednie procedury zarządzania informacjami zapisanymi w dziennikach |
| 14. | Odpowiedź jednostki audytowanej na raport i rekomendacje | Załącznik dołączony do raportu z audytu |
| 15. | Dokumenty przedstawiające realizację rekomendacji | Plany wdrożenia, poczynione zmiany w procedurach |

Przykładowe pytania kierowane do pracowników [24]:

1. Jakie procedury są stosowane?
2. Gdzie i jakie dokumenty i inne dane lub zapisy są przechowywane?
3. Jakie dokumenty są przetwarzane?
4. Od kogo pracownicy otrzymują dokumenty?
5. Jakie informacje są wprowadzane do dokumentów i skąd pochodzą?
6. Do kogo pracownicy wysyłają dokumenty?
7. Jakie metody stosują, aby wykryć błędy?
8. Co robią po wykryciu błędu?
9. Kiedy i jaki błąd pracownicy wykryli ostatnio?

# Dowody audytowe

Standardy ISACA (*060.020 Dowody*) nakładają na audytora obowiązek uzyskania wystarczających, wiarygodnych, relewantnych (powiązanych) i użytecznych dowodów, by efektywnie zrealizować cele audytu. Wnioski i rekomendacje, wynikające z przeglądu, mają być poparte odpowiednią analizą i interpretacją tych dowodów.

## Rodzaje

Można wyróżnić wiele rodzajów dowodów audytowych w zależności od przyjętej klasyfikacji (stopnia wiarygodności, źródła, formy). Generalnie przyjmuje się, że dowody pochodzące od strony trzeciej (z zewnątrz) są bardziej wiarygodne niż te uzyskane od strony zainteresowanej. Dowody materialne mają większą wartość niż informacje zgromadzone w trakcie wywiadu.

Można wyróżnić następujące rodzaje dowodów:

1. **zaobserwowane procesy i istnienie przedmiotów materialnych** — informacje zebrane w wyniku obserwacji określonych procesów oraz inwentaryzacji zasobów będących w posiadaniu jednostki;

2. **dowody dokumentacyjne** — dokumenty w formie elektronicznej i papierowej z badanego systemu oraz rejestrów dokumentów (dokumentacja systemu, wyciągi z rejestrów kontrolnych lub dziennika operacji użytkownika, faktury, zapisy transakcji);
3. **świadectwa reprezentujące** — reprezentacje jednostek audytowanych (spisane polityki i procedury, schematy systemowe, oświadczenia w formie pisemnej lub ustnej);
4. **analizy** — dokumenty będące zapisem wyników analizowania informacji za pomocą techniki porównań, kalkulacji, symulacji (porównanie kosztów eksploatacji systemu informatycznego w odniesieniu do podobnych jednostek i zbliżonych cen rynkowych).

## Forma

Zgromadzone dowody powinny zawierać:

- informację identyfikacyjną jednostki audytora,
- identyfikator audytu,
- datę pozyskania dowodu,
- identyfikator audytora.

Sporządzone przez audytora kopie muszą być oznaczone unikalnym (w ramach danego audytu) numerem dowodu, datą pobrania i nazwą prowadzonego przeglądu.

## Sposoby gromadzenia

Gromadzenie dowodów audytowych jest niezwykle istotnym i pracochłonnym elementem zadania audytowego. Nie wystarczy wydać opinię, trzeba umieć udowodnić jej prawdziwość.

W zależności od rodzaju systemu informatycznego, objętego badaniem, audytor powinien wykorzystać odpowiednie techniki gromadzenia dowodów audytu. W trakcie przeglądu można wykorzystać następujące metody:

- wywiad,
- obserwacje,
- inspekcje,
- poświadczenie (potwierdzenie) pozytywne i negatywne,
- powtórne wykonanie operacji,
- monitorowanie.

## Próbkowanie audytowe

Ze względu na złożoność systemów i mnogość przetwarzanych transakcji zwykle audytor systemów informatycznych nie bada wszystkich dostępnych informacji. Poprawne wnioski mogą być wyciągnięte z wykorzystaniem próbkowania audytowego. Polega to na zastosowaniu procedur audytowych do mniej niż 100% populacji, co pozwala ocenić dowody audytowe w sposób szybszy i mniej pracochłonny oraz sformułować wnioski dotyczące całej populacji.

Zgodnie z wytyczną *060.020.040 Próbkowanie audytowe* [50]:

> Używając zarówno statystycznych, jak i niestatystycznych metod próbkowania, audytor systemów informatycznych powinien zaprojektować i wybrać próbę audytową, wykonać procedury audytowe i ocenić wyniki próby, by uzyskać rzetelne, właściwe i użyteczne dowody audytowe.

Istnieją cztery metody próbkowania:

1. Próbkowanie statystyczne:
   - **próbkowanie losowe** — wszystkie kombinacje jednostek wybranych z danej populacji mają równe prawdopodobieństwo wyboru;
   - **próbkowanie systematyczne** — zastosowanie stałego interwału pomiędzy wyborami, przy pierwszej jednostce wybranej losowo.

2. Próbkowanie niestatystyczne (szacunkowe):

- **próbkowanie na chybił trafił** (*haphazard sampling*) — wybór jednostek bez użycia technik strukturalnych i bez świadomego przewidywania lub uprzedzenia;
- **próbkowanie osądowe** (*judgmental sampling*) — selekcja jednostek z wykorzystaniem uprzedzenia do próby (np. wszystkie jednostki o określonej wartości, wszyscy nowi użytkownicy).

Próbkowanie statystyczne, dzięki zastosowaniu odpowiednich technik matematycznych, pozwala wyciągnąć wnioski na temat całej populacji. Metody próbkowania niestatystycznego nie umożliwiają ekstrapolacji otrzymanych wyników na 100% populacji, gdyż w tym przypadku wykorzystana próba nie jest reprezentatywna dla wszystkich transakcji.

**Wskazówka!**

Jednostka próbkowana — **w zależności od celu próbkowania może to być zdarzenie, transakcja (np. dla potrzeb badania zgodności mechanizmów kontrolnych — *compliance testing of controls*) lub jednostka monetarna (np. do celów testowania dowodowego — *substantive testing*).**

Próba reprezentatywna — **wszystkie próbkowane jednostki w populacji mają takie samo lub znane prawdopodobieństwo bycia wybranym.**

Populacja — **zbiór danych, z którego audytor systemów informatycznych dokonuje wyboru próby.**

Stratyfikacja — **technika przydatna przy skutecznym projektowaniu próby; polega na dzieleniu populacji na subpopulacje o podobnych cechach w taki sposób, by każda jednostka mogła należeć tylko do jednego stratum.**

Wielkość próby — **zależy od poziomu ryzyka audytowego (ryzyko wrodzone + ryzyko kontroli + ryzyko detekcji), które audytor ma zamiar zaakceptować.**

Ryzyko próbkowania — **określa prawdopodobieństwo, że wnioski audytora, sformułowane na podstawie wybranej próby, będą**

**różne od opinii wydanej w przypadku przebadania całej populacji. Można wyróżnić tu *ryzyko niewłaściwego przyjęcia* (nieprawidłowości, którymi obarczona jest populacja, zostały uznane za nieprawdopodobne) oraz *ryzyko niewłaściwego odrzucenia* (błąd jest uznany za prawdopodobny, choć populacja nie jest znacząco obarczona nieprawidłowościami). Ryzyko próbkowania powinno być rozważane w relacji do modelu ryzyka audytowego.**

Dopuszczalny błąd (***tolerable error***) — **maksymalny błąd, jaki audytor zamierza zaakceptować, by potwierdzić osiągnięcie celów audytowych. W przypadku testów zgodności jest to maksymalny współczynnik odchylenia od przyjętej procedury kontrolnej, natomiast dla testów dowodowych błąd ten wynika z profesjonalnego osądu audytora na temat istotności.**

Oczekiwany błąd — **podczas określania oczekiwanego poziomu błędów w populacji audytor powinien wziąć pod uwagę poziom błędów wskazany w trakcie wcześniejszych audytów, zmiany w procedurach organizacji oraz dowody pozyskane z oceny systemu kontroli wewnętrznej. Większy oczekiwany błąd wymaga przebadania większej próby niż w przypadku gdy audytor nie spodziewa się błędów, by stwierdzić, że rzeczywiste błędy istniejące w populacji są na poziomie nie wyższym niż zaplanowany dopuszczalny błąd.**

Jeżeli w trakcie próbkowania zostaną stwierdzone nieprawidłowości, należy je zbadać. Jeśli otrzymane wyniki wskazują taką potrzebę, można rozszerzyć wielkość próby aż do zbadania całej populacji. W przypadku gdy nie wykryto błędów, nie należy rozszerzać próby. Audytor powinien znać techniki próbkowania statystycznego, lecz stosować je tylko, kiedy są dostosowane do obiektów i celów audytu (np. gdy chce wydać niepodważalną opinię na temat systemu, musi poprzeć ją odpowiednimi dowodami, wynikającymi z badania próby reprezentatywnej).

Więcej informacji na temat metod próbkowania wykorzystywanych w procesie audytu można znaleźć w publikacji [24].